



MAY 20, 2020

TRANSCRIPT FROM CNAS TECHNOLOGY & NATIONAL SECURITY PROGRAM EVENT

Virtual Panel Discussion on Emerging Concepts in Joint Command and Control

Transcript from a Virtual Panel Discussion on Emerging Concepts in Joint Command and Control

I. Opening Remarks

Paul Scharre: Hello, everyone. Welcome. I'm Paul Scharre. I'm a senior fellow here at the Center for a New American Security, and I direct our Technology and National Security Program. I'm very excited to welcome you today to our webinar on emerging concepts in joint command and control. We're joined here today by the Honorable Robert O. Work, former Deputy Secretary of Defense, and my colleague, Chris Dougherty, senior fellow here at CNAS on our defense team and a former Pentagon official.

II. Expert Discussion

Paul Scharre: Well, let's get right into it. Today's discussion on emerging concepts in joint command and control is motivated by a couple factors. One is the threat. The National Defense Strategy highlights our current ways of warfighting are not working anymore any we need to find ways of changing. Command and control is right at the heart of this, that we're seeing adversaries find ways to damage our ability to sense the adversary, communicate among ourselves past targeting data, and then effectively prosecute targets.

Paul Scharre: The second is really an opportunity, that we're seeing dramatic changes in digital technologies, electronic warfare, cyber, networking, data, data processing, automation, AI, all of these having significant effects on command and control. Then the third is that we've seen some early DOD efforts to grapple with some of these changes in command and control, whether it's Army efforts and multi domain operations, or joint all domain command and control across the force. So, we're seeing really a potential for some significant shifts in command and control in the years ahead, threats that we need to respond to, and opportunities as well.

Paul Scharre: So, I want to kick things off by turning it over to you, Bob. We've seen the Chinese invest in a whole slew of capabilities to disrupt U.S. command and control. What are you seeing, in terms of the threat picture and things we need to respond to?

Robert O. Work: Thanks, Paul, and good morning, everybody. It's great to be here. First, I'd like to say that we're shifting into a new era of warfare which the Joint AI Center refers to as algorithmic warfare. Just to make sure everybody understands what I'm talking about, I'm just going to read what we think algorithmic warfare means. The Chinese refer to this as intelligentized combat operations, but both of us see the same way. This is combat operations invested with intelligent weapons and equipment platforms using artificial intelligence as the core, and with the technical support from information networks, big data, cloud computing, the Internet of Things, and intelligent control. The main characteristics are intelligent ordinance, platform systems, command decision making, logistics, and equipment support.

Robert O. Work: Now as we move into this era, our conception of C2 has to change in some way. There will be much more machine intelligence in our command and control systems. There'll be much more autonomy, and we're going to have to figure out the limits of human-machine collaboration. Both the Chinese and the United States are starting from roughly the same position.

- Robert O. Work: Now the Chinese believe that the way they will beat Americans, unless... In fact, their entire theory of victory is based on what they refer to as system destruction warfare. They will try to de-link our battle networks, to disassemble them, what the Army calls disintegrate. That's how they think they will get an advantage.
- Robert O. Work: United States says we have an advantage right now in joint command and control. We've been practicing joint command and control since 1986, for certain, in both combat operations and in peace time operations. We believe that the Chinese are trying to duplicate this. But we believe, and I believe this is correct, we know joint command and control and have practiced it much more than the Chinese. So, the threat, where we're going is the Chinese say, "We want to break apart your battle network." The U.S. is saying, "We have an advantage in joint command and control. We're just going to step on the accelerator and increase that advantage." So, we're in a competition, and it's going to be interesting to see how this plays out.
- Paul Scharre: That's great, Bob. That's a very helpful overview, and I think that's a great point that the U.S. has, of course, tremendous amount of real warfighting experience over the last few decades, that's a huge asymmetric advantage of the U.S., and certainly in the conversations that I've had with Chinese counterparts on military technical issues like AI, that advantage is not lost on them.
- Paul Scharre: Chris, let me turn it over to you. How do we operationalize some of these concepts and seize these opportunities and begin to change how we do command and control to build on some of the advantages that we already have?
- Chris Dougherty: Thanks, Paul. Good morning, everybody. I'd like to follow up on what Bob said as kind of a segue into what I like to talk about, and that is that the United States and China are starting at roughly the same place, but starting with radically different perspectives on how to execute joint operations in this environment. I believe as Americans, our idealized format of this would be some form of what we might call mission command where we kind of enable... We provide a commander's guidance, commander's intent to subordinates, and then the subordinates execute with their own initiative based on that intent.
- Chris Dougherty: Now to the extent that we've actually executed that over the last 20 years of combat operations, I think a lot of people would say we haven't actually practiced what we preach. We need to get back to that. But nevertheless, that's kind of the idealized format in our head. For the Chinese, it's very different. I think they've got a much more controlled and centralized concept of C2. So, you see this emerging environment from two very, very different perspectives. The Chinese theory is that, as Bob said, we can disrupt our systems and we can maintain our own by being extremely centralized and very in direct control from CMC down to the theater command down to tactical commanders.
- Chris Dougherty: I think what's interesting is that when you try to operationalize this, you end up with very, very different answers if you think about it from those different perspectives. So, from the one side, what you're trying to do is create a very, very resilient way of doing exactly what you're already doing. I'm going to centralize this and I'm going to create multiple pathways through which I can get my centralized command and control from me at the CMC all the way down to the person at the tactical edge.

- Chris Dougherty: I think what we have to do as the United States is think about this from a different perspective. We need to kind of double down on mission command, and I think we need to accept that communications are going to get tested and integrated. So the way to operationalize this is to make that function much more resilient in terms of communicating the commander's intent, communicating a common operating picture, and allowing people down kind of lower echelons at the tactical level to execute on their own initiatives, because otherwise I think it's going to be far too difficult based on the asymmetries in geography and technology for us to try to do what the Chinese do. I think that's a failing strategy for us.
- Paul Scharre: Thanks, Chris. That's a key point that we're going to be fighting degraded. They're going to be fighting degraded, and there are areas where if we practice that, if we train for that, if we have the right doctrines in place, I would argue we have significant advantages in our ability to do so and to trust our subordinates and allow them to more flexibly adapt on the battlefield.
- Paul Scharre: Bob, what's your take on how the Department has been doing so far in some of these efforts to respond and change how we're doing command and control?
- Robert O. Work: Well, it's early days, but there is a lot of activity going on. So the Department clearly has said we want to build on our advantage in joint C2, and we want to expand that advantage into what is now called multi-domain C2, which adds space, cyber, the electromagnetic spectrum, and the information domain to the traditional domains of air, sea, undersea, and land. The thinking here is that we should be better, because we are already more versed in joint C2, we think even though we're starting at the same kind of start line, that we will be able to move ahead faster than the Chinese in multi-domain command and control.
- Robert O. Work: Now it seems to me the near-term focus is very practical. It's focused on things that we know we can do, and we do pretty well already. That is improve sensor to shooter lengths in the command and control of closing kill-chains. This all has to do with our view of multi-domain operations, and what we want to do is be able to do cross-domain effects. So, the command and control will say, "Okay, in this instance, we want to apply effects from space for this air problem," or, "We want to apply effects from the sea for this land problem." So, you see a lot of activity in this.
- Robert O. Work: The long-term focus is really on autonomy and... General O'Shaughnessy just the other day, he's the commander of Northern Command, said, "Look, the secret sauce of this is going to be predictive analysis, being able to understand what's happening and predict what may happen within 24 and 48 hours and base our plans on those predictions." The thinking is that artificial intelligence will improve slowly over time. That will allow us to do better and better predictive analysis, which will give us a decision advantage.
- Robert O. Work: Now in the Army, you see IBCS, that's their integrated air and missile defense battle command system. They're trying to link all of their sensors, their radars with Navy sensors and Marine Corps sensors and Air Force sensors, and being able to do the sensor to shooter kill chains in integrated air and missile defense. They also want to expand that. They have a technology demonstration program called Project Convergence where they're going to try to demonstrate their ability to do this in real time. The Air Force, of course, has the Air Battle Management System, which is really tied to the JADC2 joint all domain command and control. That's also very focused on closing sensor to shooter links.

- Robert O. Work: The Space Force now has an enterprise data strategy for multi-domain ops. What they want to do is build a unified data layer starting first with space data but including all sensors into a gigantic library, which they refer to as DataONE. Then there's a whole lot of activity going on in nuclear command and control and communications. So, there's enormous activity going on right now. I think what we're getting into is a phase of test a little, learn a lot, move forward, test more, add more, add in more autonomy, add in more AI-enabled capabilities. Check out the limits of human-machine collaboration, and go as fast as we possibly can. Our judgment, Paul, is that we will move faster than the Chinese in this regard because of our long experience in joint command and control.
- Paul Scharre: That's wonderful. We've had a whole bunch of questions come pouring in, and these are excellent questions. So, I'm going to turn and start bringing them out to you guys. Let's start first for you, Chris, what are the best current or historical examples of mission command and distributed execution being operationalized with success? What lessons do they suggest for how we should approach the current challenge we're facing?
- Chris Dougherty: The example I really like to go back to Martin van Creveld's *Command in War*, sort of the classic book on this topic. The two examples he brings out in that book are the German military kind of post-World War II, and then Israeli military, the IBF sort of 1950s to 1970s. The best examples of it is that it gives you a great degree of tactical and operational flexibility. It allows you to operate with a great deal of resilience when structures are attacked or cut off, and it allows you to move much more rapidly than your adversary if your adversary has got a more rigid, hierarchical command and control structure. The class case study in this being the Battle of France in 1940. Anybody who's read Marc Bloch's *Strange Defeat*, in which he talks about how the Germans could just move so much faster than the French is sort of the classical case study of this.
- Chris Dougherty: The downside to that kind of command structure is that it can create operational flexibility sometimes at the expense of strategic direction, and the study of that is World War I, the Germans had a great deal of operation success on the western front in early 1918. It was toward no particular end really whatsoever. They found that they were just sort of throwing good money away. In the end, it petered out and had no real strategic impact.
- Chris Dougherty: So I think the question we have to think of is if we're going to think of these case studies, how do we take the good things about operational mission command that gives us the flexibility, but maintain that overall direction, the strategic direction at the high levels of command so that we're actually coordinating our efforts toward the objectives that we care about.
- Robert O. Work: Hey, Paul. This is Bob. Can I add something?
- Paul Scharre: Yeah, by all means.
- Robert O. Work: The Chinese have this right. I think we're moving into this era of what they refer to as systems confrontation, which are these big collisions of what we refer to as battle networks and they refer to as operational systems. The Russians refer to them as reconnaissance strike complexes. So, in this question, what we need to look for is mission command within a battle network type of example.

- Robert O. Work: The best one for me, even though it's dated, is the British integrated air defense system in 1940. It was called the Dowding system. What it was, of course, it had a sensor grid with radars that could look far and radars that could look on the deck. It had Royal Air observers. They would pour all of their observations into what was called a filter center at Bentley Priory. Bentley Priory would create what was called, and I love this term, a common recognized operational picture. The recognized operational picture was the commander telling the force, "Whatever you see in your sector, I am telling you what is the common recognized operational picture, and I will tell you what is the major attack that we together must beat. Then from that point on, giving mission command orders to the fighter sectors and the fighter squadrons."
- Paul Scharre: Everything synced up, and it synced up rapidly every time the Germans tried to send an attack. So, mission command to me means that you really only have to transmit two things to the force. The common recognized operational picture, the picture that the commander in charge says, "This is the picture that I am working on." The second is commander's intent. If your force is trained to operate with that data, then you will have a self-synchronization even when the individual elements of the force don't have communications to higher command authority. So, when we think about mission command, we need to think about mission command within the framework of our battle networks that we fight in now as a joint force.

III. Audience Q&A

- Paul Scharre: We have a whole bunch of really good questions queued up here. I think we've got about nine in the queue and more coming in. I'm going to combine a couple of them, because I think some of these hit on similar themes. One of them is about cyber capabilities. So, if we connect everything, then a cyber weapon could spread everywhere to a catastrophic effect on our systems. What's being done to defend against that threat.
- Paul Scharre: Let me sort of add into that a related question about how we're responding to the accelerated pace of tempo in current operations due to future capabilities and threats. So how will emerging joint C2 initiatives address 21st century operational speeds presented by hypersonics, satellites, cyber space threats? What DOD doctrinal, organizational, or training changes might be needed? So how do we think about some of these new threats and capabilities as we're implementing these new command and control concepts?
- Chris Dougherty: I think the first question about cyber is certainly a concern. Yeah, it's hard to discuss exactly how you would defend against that in an unclassified setting, but I think one of the things we could probably think of is how do we maintain a level of connectivity across the joint force while still hiding off certain parts of insecurity perspectives so that one infection in one part of the network can't suddenly infect the entire network.
- Chris Dougherty: So, one of the things we've discussed in the C3 level is having the ability to multi-path data around the network without the various parts of the pathways actually being able to read or understand the data? So, if I need to talk to Paul, but I need my data to go through Bob, what I can do is I can pass data from Bob to Paul, but Bob's system may never actually read the data. Meaning that if there was malware in there, it might not actually infect Bob's system. It might infect Paul and me, but hopefully the entire system wouldn't go down. That's one kind of method we could do to resolve that question.

- Chris Dougherty: The second part is interesting and something that I've spent a lot of time thinking about, which is the speed of 21st century operations. I think one of the critical aspects of that is we've got to figure out how to, as Bob puts it, manned-unmanned teaming, but I think how do you lash up unmanned systems and artificially intelligent systems with humans to enable them to do what they do well, which is large-scale pattern recognition and enable humans to do what we do well, which is sort of rapid decision-making within that structure. I think that'll be the secret sauce to whoever figures out this future competition is the side that understands what's the right mixture of technology and humanity to solve that particular question.
- Chris Dougherty: One of the things I will say that concerns me most of all is that a lot of its preparation. If you look at what the Chinese and the Russians are doing in this space, they focus a lot on preparing the battle space in the information domain. They focus a lot on... The Russians like to call it the initial period of war, but their belief is that if you don't start acting preemptively and preparatively, that you're going to be behind the eight ball when all of these things start kicking off.
- Chris Dougherty: So, the difficulty from our perspective is that we don't tend to focus our efforts on those sorts of preparatory actions the way we might want to, because our attention is global. We're focused on a wide variety of threats. So, the question for us is how can we actually think about taking preparatory steps? How can we get the right authorities to do those sorts of things in the theaters that we care about? Because otherwise if you wait until the war has started, it's going to move too fast for you to get ready.
- Robert O. Work: Yeah. On this, Paul, we need to get the Department of Defense. I think the Department of Defense needs to get more literate in the fundamentals of algorithmic warfare. The Chinese write a lot about this. Now whether or not they're better and worse than us, they do write about it a lot more than we do, and they think about it. Algorithmic warfare, they state it boldly. The winner will have algorithmic superiority. In cyber, we must have better algorithms than the Chinese. If we don't, we are going to be in a world of hurt. These must be autonomous cyber systems that can sense the attack and immediately start fighting it back without any human intervention. It's got to move at machine speeds. We already know humans are incapable of keeping up with a machine-generated cyberattack.
- Robert O. Work: So, it's why in cyber we must have better algorithms. The same goes for electronic warfare. We're doing a lot of research in what is called cognitive EW, where the machine is able, in real time, to beat back waveforms that it hasn't seen before and find parts of the spectrum where we can still operate in and pass data as needed. Now we're in early stages here. This is a competition. The Chinese are pushing hard, in terms of the offensive cyber, and we need to really push hard, in terms of the defensive, and, of course, we need to have our own offensive capabilities also.
- Robert O. Work: This is all about battle network defense. The Chinese actually have added a fifth grid to the four canonical grids of a battle network. Sensor, command, control, communications, intelligence, effects, and sustainment regeneration. They call it information contestation grid. It is consistent with their theory of war where they're going to go after our network in a wide variety of areas.

- Robert O. Work: So, am I confident we're going to come out on top in this competition? No, I'm not yet, because I don't think we are paying enough attention to it. But the question is a good one. We will be more vulnerable to cyberattacks than we have in the past. We need to prepare for that future.
- Paul Scharre: This is an interesting area where there is so much commonality that I often see between how the Chinese are writing about, say, artificial intelligence and technology in war. A lot of that is not a surprise. They are reading what people are writing and thinking here in the United States, and they're mirroring it back. But one of the areas where I have noticed a significant difference is what you were saying, Bob, which is really a greater focus in Chinese writings and thought on command and control. I think that they are, in retrospect, probably right to make that a priority area, that there are very significant changes that we're seeing in EW, networking, ISR, algorithms, all of which have really big potential to change command and control.
- Paul Scharre: We've got a related question that really gets at this issue of human-machine teaming and algorithms that we've been talking about. It's a great question here. It says, "How much of mission command is about education, training, readiness, and having adaptable war fighters, and how much is about the algorithms? Do we have to have smart decision makers in the battlefield or effective button-pushers and smart machines? How much of our scarce dollars should go to each of those respective areas?" Chris, why don't you start? What do you think?
- Chris Dougherty: I think Bob and I are going to have pretty different answers to this. I think I would probably put most of my money toward the people, at least now again I'd say most of my research is done roughly the 10-year time frame. So, it's within that time frame, I don't think that a lot of these intelligence systems are going to be quite as capable as we might wish them to be. I think there's going to be still a lot of work to be done within 10 years, in roughly 2030. So in that period of time, I think it's going to be the onus of mission command, the onus of effectiveness in these competitions is going to fall a lot on human decision making.
- Chris Dougherty: In that place, I think it's actually an advantage that we have over the Chinese, and they recognize this, as you mentioned, Paul. They write extensively about their shortcomings in command and control. They write extensively about shortcomings in their junior officer corps and their ability to take initiative in testing environments. It's something they're well aware of. They're trying to work to fix, but it's a very, very difficult thing to fix. So, I would say from an American perspective, our secret sauce in this competition ought to be our people, and I think we ought to invest in training and developing the unit cohesion.
- Chris Dougherty: One of the things that we talked about earlier and I wanted to bring up was we've talked a lot about how we're good at joint command and control. I'd argue actually we're kind of good at adjacent command and control. We don't really conduct joint operations. We conduct operations that look sort of joint, because we're all kind of adjacent to one another. But when it comes down to actually functioning jointly, it only happens at very, very high echelons of command with very certain exceptions, maybe in the special operations community and a few other places. But by and large, everything occurs inside service stovepipes.
- Chris Dougherty: So, the difficulty with moving towards something like multi-domain operations is we have to break that down. Part of that's a technical challenge, but a huge part of it is an organizational

and training challenge. It's one thing to say, "Well, I'm going to allow Bob to control Paul's assets in a tactical environment, because Bob has a better operational picture and Paul has the missile that he needs." But if you two don't trust each other and you two don't know each other and you haven't trained together to do that, achieving that level of decentralized control is going to be really, really, really hard. Achieving the level of trust necessary to do that is going to be virtually impossible. So, I think we need to think differently about how we train and organize our forces and not just necessarily how we equip them to do this so that we can actually achieve that level of effective mission command.

Chris Dougherty: Now here Bob's going to tell you why the machines and the algorithms matter much, much more.

Robert O. Work: No, I'm not. I would never say something like that. I would also point out that commandant just wrote an update to his planning guidance that said, "Training and education is the number one priority." Look, a lot of people thought that the Third Offset was all about technology and machines and robots and stuff like that. The Third Offset adopted the definition of autonomy that was put out by the C2 division in the John Hopkins Applied Physics Laboratory. Let me just read it for everyone.

Robert O. Work: "Autonomy is not a technology. It is a command and control approach that seeks to push power and decision making to the warfighting edge, and the capability of an individual element in the force to operate without communications to a command authority." The Third Offset was about making that vision happen. I agree totally. This is more about our commanders. In the future, if all we have are commanders who listen to a recommendation from an algorithm and always hit the "I believe" button and go, we don't need humans. Just go to the algorithm. We want commanders who will say, okay, this was just another input that I am going to sift through my own experience and I'm going to make a decision that I think is most consistent with the common relevant operational picture and the commander's intent.

Robert O. Work: So, this is all about the people and understanding how people work with machines and use the advantages of both to have better combat outcomes. So, I agree totally with you. This is about people.

Chris Dougherty: Just to two-finger that, I know, Bob, you're familiar with this, but one of the critical aspects of the Second Offset was the development of improved training capabilities. In particular, I'm thinking of things like miles, things that Paul and I probably took for granted when we were in the Army, the National Training Center, other things like that, right? Which now we think of as kind of antiquated and almost silly, but at the time, they were radically transformative to how we did combined arms training. It allowed us to take the aspects of the Second Offset and actually train our forces to be ready to use those technologies in the event that we had to fight the Soviets.

Chris Dougherty: I think what we have to think about is if we're going to implement this new kind of warfare, we're going to need new kinds of training. I think the old ways we train don't really work, because we can't incorporate all of these different domains into a training site. So I think we're going to have to figure out how do we mix live actual physical exercises and training with synthetic training so we can create these commanders who are capable of operating functionally multi-domain inside their own minds, because if you read Chinese and Russian

doctrine, they're very, very explicit about how they want to use technology to exploit cognitive weaknesses. They want to overload you cognitively so they don't have to beat you physically. I think we have to figure out how to train ourselves to be ready for that. It's a really, really hard thing to do.

Robert O. Work: I agree. All of that training was basically based upon the idea of force-on-force training. We now have to do network v. network training. In every single exercise, we should have a world class cyber electronic warfare system destruction unit, like the aggressors out at NTC, the National Training Center. All they're doing in every exercise is trying to knock down our network and see what happens. We should never allow a reset in a network to say, "Oh man, we're not communicating with each other, so let's reset and start again." We'll never train the force to do mission command and to operate without communications to hire unless we do that.

Chris Dougherty: We held a wargame remotely a few weeks ago, and we were still working through some of the technical difficulties of doing something. We were running it simultaneously over Zoom and Slack and Google Docs and PowerPoint and you name it. We had all these different platforms, and the blue team lead said to me, he said, "This is a great game for a lot of reasons." I said, "Yeah, I wish the tech would work a little bit better." He said, "Actually, the tech was great, because," he said it reminded him of actually being in command with all of the difficulties of getting all the networks to connect to one another.

Chris Dougherty: He said, "Even better, next time you should make it harder." He's like, "You shouldn't tell any of us how this works, and just let us figure it out." I was like, "Wow, okay. Maybe I will try that." I don't know if I could get the effect I want, but nevertheless, I thought it was really interesting that he found there's an educational training value from just having to work through the friction of it.

Paul Scharre: A bit of a meta game there. Well, we got a question that really builds on this, I think, in a really helpful way. You were talking, Bob, about some of the challenges that some of these exercises have been canned in the past that we just reset the network and start again. We got a question about how we actually try these things out and learn. We are largely talking about theoretical and speculative concepts of warfare, which you've not really seen before in the real world. Certainly, I'll point out that's true for any time we have some new technology and new ways of fighting that we're trying to integrate into the force.

Paul Scharre: So, the question is how do we begin to explore how we use these theoretical concepts and how we apply them in the real world?

Chris Dougherty: I'll jump in here. I'm a huge advocate of Peter Perla's work on the cycle of research. I think that's probably the way that I would go about doing this. Don't reinvent the cycle of research. Just use it. But by that, I mean I think the way you start is with wargaming and various other forms of exploratory work to kind of find out if there's a "there-there" with the concept. At a low level of investment, the wargames are relatively affordable. It allows you to kind of understand does this actually look like there's something there.

Chris Dougherty: Then you move on to a little bit more detailed technical and physics-based models and mission models to really explore, okay, now I think there's a "there-there," and how robust is that there? Then you take that, and you exercise it in the field with things, like various test

ranges. You say, “Okay, this is actually when I took this idea, I modeled it, and then I turned it into a real widget. Can I actually use that in the field? How hard is that?”

Chris Dougherty: Then you say, “Okay, it's not the end of it, right? It's a cycle.” So, you go back and say, “Okay, it turns out that maybe I can't actually communicate with all of my sensors in this particular way. Is there something else I could do?” Then you keep doing it and you keep iterating. The good thing about that is it allows you to keep working and grinding on a problem in kind of these little bits and pieces, like you said, all to eventually arrive at a better conclusion.

Chris Dougherty: The difficulty I think for us in this regime is that what you're doing is you're constantly iterating around a bunch of systems that need to link together. One of the things we found historically with this problem set is that you're trying to develop a new architecture and a new way of doing business in the command and control regime and communications regime, but you also have a huge legacy force behind you, but you have to figure out, “I can't build a new regime that none of that can participate in.”

Chris Dougherty: One of the ways we've done in the past is we've enforced things like backward compatibility, interoperability so that everybody who's got a radio from even 30 years could still participate in this network. We found that's actually incredibly difficult and incredibly costly. So, one of the things we're going to have to figure out with things like JBMS and JADC2 and all those sorts of things is how do all of the older systems and how do the systems possessed by our allies and partners, how are they going to plug into this network?

Robert O. Work: Well, Paul, one of the big things we need to do is we need to free up slack in the force for us to be really training hard on this all the time. We need to rethink... We really value forward presence for good reasons, but it's very, very expensive and nearly all of our ready forces are out all the time doing presence missions. We need to value training the force in this way of warfare as much as we value forward presence. We have to have more units staying back on the ranges doing localized experimentation. We need to ask the NTC, the National Training Center, Red Flag and Top Gun, all the COMPTUEXs need to say, “There has to be a network v. network component in everything we do. There are no resets. We're going to give you a world class opposing force, a network OP4 that's going to be spending all of its time trying to knock you back on your heels, and we just have to inculcate this throughout the force.

Robert O. Work: That's the only way we're going to get to this mission command type stuff, because I agree with Chris. The last 17 years, because technology allows higher echelons to reach deeper and deeper into the force, we have to walk back bad habits, I think, and really get back into walking the way we talk. So, to me, this is really a commitment by the Department of Defense and the whole joint force to say, “Look, we're headed towards this future.” This is kind of like aviation in the inner war period. Everyone knew that aviation was a good thing, and everyone knew that aviation was going to have an enormous impact on the way the Navy fought. But everybody had a different idea of what that impact might be.

Robert O. Work: So as Chris said, they would do wargaming up at War College. Then they'd do a fleet exercise and they'd test it. Then they would feed it back into the wargaming. We need to get back to that kind of a cycle, because I think everyone would say we know artificial intelligence and autonomy is going to change the way we fight. We're not really certain how it will, but we

know it will, so let's start doing the incremental wargaming, experimentation, exercise, and learn as we go, and learn faster than the Chinese or the Russians.

Paul Scharre: Let's talk about where the rubber really meets the road here, which is funding. I got a couple questions about budget issues that I think are great and really build on this very well. So, one is JADC2 requires all services to buy in to include funding. Now typically horizontal programs, those that affect all the services, are tough to gain service funding support. So how does DOD encourage services that they must support these multi-service efforts. So that's one question.

Paul Scharre: But a related one, which gets to a bit of a higher level of the funding issues here, which is that developing C2 will require experimentation, constant development, acquisition, as we've been talking about. All of this requires additional resources, but in the post-COVID world, DOD might have to make do with fewer resources. That's an assumption, but I think that's a fair one that as we see the government take on increasingly significant amounts of debt, as we look into the years ahead, we may see greater downward pressure on DOD's budget. So how can DOD find more resources for C2 initiatives in this budget-constrained environment?

Robert O. Work: It's all about prioritization. The point is that's what I always hear and that's generally what you hear. Hey, if you want us to prepare for this new way of war, you need to give us more money, because we're doing all the old shit, and we don't want to stop doing it. It's all about prioritization. So, to me, this has to be top-down driven and it has to be driven ruthlessly in the program.

Robert O. Work: Now Secretary Esper said, "I want a joint warfighting concept, and I want it by December." He's assigned that task to the J7. They just had a TTX last week where they were exploring this. So, the thinking, at least in Secretary Esper's mind as expressed in the press, is that he wants the joint warfighting concept to be the basis for all JROTC decisions, and the basis for joint force experimentation. So, in an ideal world, the J7 will come through with an operational concept that's not going to be fully baked. It's not going to be perfect, but it will establish the framework for us going forward.

Robert O. Work: Then I would hope that the JROTC then starts grading all of the systems, the command and control systems, and saying, "You prove to me that your command and control system is consistent with the joint warfighting concept," which is going to have a really, really important JADC2 component. Then within the program, you should see more money for experimentation and more money for exercises, etc. now that's got to come from somewhere in a constrained top line, but that's what we have to do if we believe that we're moving into a future where the character of war, not the nature of war, but the character of war is fundamentally changing. So, you better get ready for it, or you're going to be left behind.

Chris Dougherty: Bob, I thought you were going to reference the need to have OSD create pockets of cash but incentivize innovation, but it's something we talk a lot about, and I think it's critical that we... There's two ways to go about doing this. One is you can mandate from the top-down from OSD and say, "Thou shalt build this." Another way is to create a pool of cash that says, "Look, whoever gives me a good concept, a good suite of capabilities for how we're going to do this thing, you can capture this suite of cash, and it can go into your top line,"

but again, that requires a certain level of flexibility inside the budget, which is both an OSD issue, but it's also a congressional issue. But I think we have to figure out how do we create incentives to do that? I would argue right now, it appears to me, just from watching what's been happening with JADC2 and ABMS, other things like that, we're actually creating disincentives for that sort of service-level initiatives rather than incentives, but hopefully it's improving over time.

Chris Dougherty: Paul and Bob, both of you, I think I've mentioned prioritization, and I have to say that in the National Defense Strategy, the highest priority investments were in creating a more resilient ISR architecture. They're kind of right up there right next to investments in our Nuclear Deterrent Force, and we recognize that because if you read how China and Russia talked about fighting us, they do not want to fight us force on force. They do not want to fight us on a level playing field. They want to knock out our eyes and ears. They want to take out our central nervous system, and then they want to pick us apart piece by piece if they have to fight us. Frankly, from their perspectives, they would rather demonstrate to us an ability to do this, to deter us before conflict even happens so that they can just do what they want to do and we don't even bother to contest it, because we know that our systems won't function in the event that they fight us.

Chris Dougherty: So, if somebody were to say to me, "I got to cut huge chunks out of DOD's budget," I would say, "Okay, fine, protect all the investments in these systems, because these are critical. We can afford to lose some force structure if we have to. We can afford to take hits other places. If we don't follow through on these investments, we'll find ourselves deeply behind in the eight ball in any kind of crisis or conflict with China or Russia, and it will be a position from which I don't think we'll be able to recover at that point, whereas I think we can probably stand to lose a little bit of investment in force structure and personnel. I think that's something we can make up in the backend. But losing this, I think would be penny-wise and kind of foolish.

Robert O. Work: Chris, you bring up a good point. You can try to do a heavy-handed OSD top-down approach, and I believe a heavy-handed OSD push is absolutely critical whenever you're trying to pursue one of these very, very, very broad transformations, but you'll go a lot faster and do a lot better if you have a bottom-up component. We saw that in the Second Offset when the top-down push from OSD was we are going to go in a deliberate way towards guided munitions and the battle networks that can employ them at range.

Robert O. Work: So, the term I liked the best was the NATO term of follow-on forces attack. We called it assault breaker. But when it really kicked off was when the Army and the Air Force got together. It was General Creech and General Starry, I think. When they got together and they said, "Let's do air-land battle together," and they agreed to 31 initiatives between the Air Force and the Army that would push it forward. So, you had this top-down push, which was very, very strong, and you had a very vibrant bottom-up. We want to try to duplicate that and having incentives in the program and the budget the way you described is one way to get there.

Chris Dougherty: The one thing I think that concerns me that I've seen is that command and control really gets to the heart of... I don't want to go all Masks of War, but I think it gets to the heart of how military services see themselves. I think it's very difficult for us to come up with a truly joint command, control, and communications architecture that services all of these

different... That provides command and control to all of these different services and all these different domains in a way that actually conforms with their self-conception of their own command and control, but also their conception of how that ought to be done.

Chris Dougherty: I think I saw a lot of resistance in wargames when Air Force folks would take the lead and say, "This is how we're going to do this." You would kind of see a little bit of standoffishness, frankly, from some of the other services saying, "Look, that might work for the Air Force. That might work in the air domain. That might work in space. That doesn't work down here on the ground, or it doesn't work at sea. We have all these different requirements. We have all these different demand signals. You don't understand." So, I think one of the things that concerns me is how do we come up with something that really works jointly, even though acknowledging that the Air Force is going to be the lead service proponent of it.

Paul Scharre: That's a great point, Chris. As we begin to think this through jointly, there are not just cultural differences, but there are real differences in these warfighting domains, the physical characteristics of them, the ability to move forces quickly in the aerial wing, which is certainly not the case in ground, and I'd see that changes how we think about command and control.

Paul Scharre: We are about out of time, and it's time for maybe one more question here. We're talking a lot about China. We've got a question. What are the differences and implications when we consider Russia? Chris, let's turn it over to you first.

Chris Dougherty: So, there's actually a fair degree of similarity in how they talk about it. Some of that's based on sort of their common Marxist-Leninist backgrounds way back in the day that is still the formation of a lot of the military thinking, even if they've lost some of the over references to Marxist Leninist pieces, some of the points about continual struggle and confrontation. That terminology carries over.

Chris Dougherty: Frankly, when they talk about fighting the United States, we're the same enemy. So, a lot of what they're going to talk about is going to look a heck of a lot similar because they're fighting the same group of folks. The one thing I would say the Russians are perhaps a little bit more interested in using systems to manipulate behavior, what they call reflexive control. Both sides what to use stratagems and deceptions and all that stuff. So, it's not to say that the Chinese don't do that, but it probably plays a bigger role for the Russians than it does for the Chinese. In large part, I think it's because they don't have some of the technological capabilities the Chinese do to disrupt networks at range, right? So, I think they want to use your networks against you. They know that in some cases they're not going to be able to get into your command and control architecture out several thousand nautical miles away. They want to disrupt it and kind of manipulate you to behave in ways inside the theater where they have an advantage.

Chris Dougherty: I think the big thing I think that differentiates them is that both sides see information as the domain and everything else as sort of a contributing factor to it. But for the Russians, it's very, very clearly always about manipulating you psychologically and cognitively, whereas the Chinese, as Bob says, talk a lot more about systems destruction warfare from the perspective of destroying the system or disrupting it technically. They also think about the cognitive perspective, but it's not quite to the same degree that the Russians do.

- Robert O. Work: Yeah, it's interesting. The Russians started talking about battle network warfare before we did. After the assault breaker demonstration in 1982, within two years, Soviet General Staff had concluded that the appearance of what they referred to as reconnaissance strike complexes had fundamentally changed the character of war and had completely overthrown their campaign design. They talked a lot. Their reconnaissance strike complex envisioned a future in which it would go totally automated. The Russians appear to be much, much more risk-tolerant of a totally automated system. In fact, there are indications in the open press that they've taken this into their nuclear command and control.
- Robert O. Work: I don't think the Chinese go as far as the Russians. It's very concerning if you would think about a system that could automatically trigger either a preemptive or a retaliatory strike, and the Russians would say, "Oh sure, let's go for this system. We really understand combat to the point where we can make algorithms or functions that are scientifically based in fact and very reliable."
- Robert O. Work: So, for me, one of the most troubling aspects of the competition and algorithmic warfare is the degree to which any of the competitors will start to really rely on machine intelligence and autonomy to drive the train. There are some futures that would really cause us a problem.
- Paul Scharre: Well, we have just a few minutes left. We have a whole pile of really, really good questions that I wish we had time to get to unfortunately we're going to have to leave on the table. But I want to give you each one last chance for one minute, any parting comments. Let me ask you what do you think is the most important single thing the department should be doing to adapt this command and control for this future environment? Chris, you're up first.
- Chris Dougherty: Everything I've seen from both wargaming and modeling simulation suggests that we can change our C3 architecture all that we want, and that's certainly a good thing, and we certainly ought to do it. We certainly ought to make those investments. But the critical thing is going to be changing how we command and control forces and actually truly becoming a joint force rather than a force that operates next to each other and occasionally cooperates. I think that's going to require changing how we think about training and organizing our forces and actually truly training jointly.
- Chris Dougherty: As Bob mentioned, we got to change how we do red flag and NPC. I would argue that those need to become truly joint training exercises where you would see all domains, all services represented, and we train that way and then we deploy that way, because it's going to be too late to play a pickup game if we want to try to do that in this environment. I would say that's kind of the number one thing I would take away from this.
- Robert O. Work: I'm a little biased. Well come from where we sat. I thought we started to build some real momentum on the Third Offset strategy by 2017. But in the change of administrations when Secretary Mattis came aboard, he rightly prioritized trying to fix readiness. That was the wolf closest to the sled. He absolutely had to do that. So that turned the attention of the senior leaders of the department inward. How do we fix our mission readiness rates for our aircraft? How do we get more out of our ship maintenance availabilities, etc.? It was exactly the right thing to do, but it kind of took our attention off of the future, in my view.

- Robert O. Work: Now we're going to move into a situation where readiness is coming back. It's not nearly as far along as I think everyone would hope, but it's certainly a vast improvement over 2017. We're facing everyone, I think, I think the department is consigned to the fact that the best-case future right now looks like FY21, about 735 billion a year without inflation. That's the best case. So, everyone is saying, "Okay, we're not going to get the 3 to 5 percent real growth that we were hoping on, and all our plans were on... This is going to require really ruthless prioritization."
- Robert O. Work: So to me, this is all about, look, the prioritization has to be on training the force for getting ready for this new type of warfare and approaching, experimenting as we are doing now to try to figure out the best way to command and control a multi-domain operation in the truest sense of the word.
- Robert O. Work: So, I'm actually I'm a glass half full type of guy when I see the IBCS, Project Convergence in the Army, the JADC2 and the ABMS in the Air Force, DataONE and the unified data layer in the Space Force, and all of the things that the Navy is doing in terms of their distributed operations, etc. The Experimentation is there. It's starting to come along. So, I believe we've started. We've lost time. That's the frustrating part. So that's the glass half empty of me talking. We've lost too much time since 2017, but it really seems to me, Paul and Chris, that we've started off on the right vector.
- Paul Scharre: Wonderful. Well, we are unfortunately out of time. But thank you, Bob, thank you, Chris, for a really interesting discussion. Thank you everyone who joined us today. Thank you for those who submitted questions to really help contribute to a very thoughtful and interesting discussion here. Please stay safe, stay healthy, and all the best. Take care.